

PSP SIGNALDESK · PT PACIFIC STRATEGY PARTNERS

Déclaration de protection des données PSP SignalDesk

Comment PSP SignalDesk protège les données personnelles de ses abonnés, où qu'ils soient : rôles, données, sous-traitants, sécurité, conservation, droits, gestion des incidents, transferts transfrontaliers, desks d'administration des partenaires et loi applicable là où vous êtes.

PT Pacific Strategy Partners · Jakarta et Sydney · Septembre 2026

PT Pacific Strategy Partners, Jakarta. Version 3.0, 14 septembre 2026. Questions sur cette déclaration : privacy@pspsignaldesk.com.

1. Qui nous sommes et les rôles

PSP SignalDesk est une plateforme d'intelligence décisionnelle pour les dirigeants d'entreprise en Indonésie et dans l'ASEAN, conçue et exploitée par PT Pacific Strategy Partners, WTC 5, Jl. Jend. Sudirman, Jakarta, avec Pacific Strategy Partners, Sydney. PSP SignalDesk est enregistré comme opérateur de système électronique de portée privée auprès du ministère de la Communication et des Affaires numériques, Tanda Daftar PSE 029810.01/DJAI.PSE/09/2026.

Rôles au titre de la loi 27/2022 sur la protection des données personnelles (UU PDP) et du règlement gouvernemental 33/2026 :

- PSP est le responsable du traitement de chaque compte de la plateforme, au titre de l'UU PDP en Indonésie et de la loi de protection des données de votre propre pays ailleurs. Les abonnés activent le service et acceptent les Conditions et la Politique de confidentialité de la plateforme directement auprès de PSP.
- Lorsqu'une organisation partenaire, telle qu'une chambre de commerce ou une association professionnelle, met la plateforme à la disposition de ses membres, le partenaire ne fournit pas à PSP sa base de données de membres. Les membres activent le service directement. Les seules données qu'un partenaire transmet à PSP sont celles des personnes qu'il désigne pour des sièges de programme, fournies avec leur consentement.
- Une organisation partenaire est le responsable du traitement des données qu'elle collecte par ses propres canaux, et des informations de programme qu'elle voit sur son desk d'administration (section 9), qu'elle utilise uniquement pour faire fonctionner son programme.

2. Quelles données personnelles PSP SignalDesk traite

Qui	Données personnelles	Finalité	Base
Abonné	Nom, adresse électronique professionnelle, organisation, fonction, langue, préférences de secteurs et de marchés, formule d'abonnement et statut	Fournir et assurer le suivi de l'abonnement	Le contrat de l'abonné avec PSP

Qui	Données personnelles	Finalité	Base
Abonné	Conversations avec l'analyste, décisions enregistrées, entrées du classeur, compteurs d'utilisation	Fournir l'analyse demandée par l'abonné et conserver son propre historique	Contrat ; l'abonné peut supprimer chaque élément à tout moment
Abonné, facultatif	Numéro WhatsApp et texte des messages	L'assistant WhatsApp	Consentement, donné lorsque l'abonné relie son numéro ; retiré en le déliant ou en répondant STOP
Abonné, facultatif	Outils métier connectés : instantanés comptables (Accurate, Kledo, Xero), Google Sheets, Calendar et Drive ; documents téléversés	Analyse demandée par l'abonné sur ses propres chiffres et documents	Consentement, donné à la connexion ou au téléversement ; retiré par déconnexion
Agents d'un partenaire sur un desk d'administration	Nom, adresse électronique, rôle	Faire fonctionner le programme du partenaire	L'accord de partenariat
Tous	Journaux de sécurité et de service	Sécurité, prévention des abus, qualité du service	Intérêt légitime

Non traités : données d'enfants, enregistrements vocaux des abonnés, données biométriques, scripts publicitaires ou de suivi.

3. Où les données sont traitées : sous-traitants ultérieurs

Sous-traitant	Rôle	Pays	Conservation	Certifications
Cloudflare, Inc.	Hébergement, exécution, stockage, journaux	États-Unis ; réseau mondial incluant Jakarta	Supprimé à la résiliation ; journaux 30 jours	ISO 27001, 27018, 27701 ; SOC 2 Type II
Anthropic, PBC	Analyse par IA pour SD Analyst, SignalPulse et l'extraction de documents	États-Unis	Entrées et sorties supprimées sous 30 jours ; jamais utilisées pour entraîner des modèles	SOC 2 Type II ; ISO 27001
Meta Platforms (WhatsApp Business Platform)	Acheminement des messages WhatsApp	États-Unis et Irlande	Messages conservés uniquement jusqu'à leur remise	ISO 27001 ; SOC 2 Type II

Sous-traitant	Rôle	Pays	Conservation	Certifications
Resend, Inc.	Courriels transactionnels : codes de connexion, factures, notes	États-Unis	Journaux d'envoi 30 jours	SOC 2 Type II
Stripe, Inc.	Paiements par carte, lorsqu'un abonné paie par carte	États-Unis	Enregistrements de transaction selon le droit des paiements	PCI DSS niveau 1 ; SOC 1 et SOC 2
ElevenLabs, Inc.	Génération vocale pour l'audio éditorial	États-Unis	Scripts éditoriaux uniquement ; aucune donnée d'abonné	SOC 2 Type II
Netlify, Inc.	Hébergement des pages web	États-Unis	Aucune donnée d'abonné au repos	SOC 2 Type II

Chaque sous-traitant est lié par un accord de traitement des données en vertu duquel il agit uniquement sur instruction de PSP, n'utilise pas le contenu des abonnés pour l'entraînement lorsque l'IA est impliquée, supprime sur demande et notifie PSP de tout incident.

Ne sont pas des sous-traitants : Google, Accurate, Kledo et Xero sont des services qu'un abonné choisit de connecter, et chacun est responsable indépendant de son propre système. Les connecteurs qu'un abonné active dans son propre compte Claude, ChatGPT ou Microsoft Copilot sont régis par l'accord propre de l'abonné avec ce service.

4. Mesures de sécurité

- Toutes les données sont chiffrées en transit et au repos.
- L'accès se fait par des jetons de session signés à courte durée de vie ; les fonctions d'administration exigent une session administrateur distincte, et le desk d'administration d'un partenaire est limité aux comptes que le partenaire désigne.
- Les identifiants sont stockés avec un hachage itéré et salé par utilisateur ; des échecs de connexion répétés bloquent l'adresse.
- Les identifiants des outils connectés sont chiffrés avant stockage et révoqués chez le fournisseur lorsque l'abonné se déconnecte.
- Chaque activation, connexion, action WhatsApp, requête à l'analyste et génération de document est limitée en fréquence.
- L'assistant WhatsApp ne répond qu'aux numéros reliés, et chaque message entrant est vérifié par signature.
- Les comptes de démonstration sont en lecture seule.
- Les événements de sécurité et de service sont journalisés pour l'investigation des incidents. Aucun script d'analyse ou de suivi tiers ne fonctionne sur la plateforme.
- L'environnement de préproduction est séparé, sans donnée d'abonné et sans courriel sortant.
- Le consentement et son retrait sont enregistrés par abonné et par finalité, avec la version et la langue de la notice.

- La clôture d'un compte supprime la fiche de compte, la mémoire du desk, les conversations, les décisions, le classeur, les documents et les identifiants des outils connectés sur les systèmes de PSP sous trois jours, et les sous-traitants suppriment dans leurs délais contractuels.

Une description technique de ces mesures est disponible pour les parties contractantes sur demande, sous engagement de confidentialité.

5. Conservation

Classe de données	Conservation
Fiche de compte et contenu du desk propre à l'abonné	Durée de l'abonnement ; supprimés sous trois jours après la clôture, ou plus tôt lorsque l'abonné supprime un élément
Mémoire des conversations WhatsApp	24 heures
Données des outils connectés	Mises en cache pour la session de travail uniquement ; rechargées sur demande ; supprimées à la déconnexion
Documents téléversés	Supprimés chez le fournisseur d'IA après traitement, au plus tard sous 30 jours
Tickets d'assistance, demandes de session, réponses aux enquêtes, retours	Durée de l'abonnement ou du programme partenaire plus 12 mois
Compteurs d'utilisation mensuels montrés à une organisation partenaire	16 mois
Factures et enregistrements de paiement	10 ans, comme l'exige le droit indonésien
Journaux de sécurité et de service	30 jours

6. Vos droits et comment les exercer

Vous disposez des droits que vous confère la loi de protection des données de votre pays. Au minimum, où que vous soyez, nous vous accordons : information, accès et copie, rectification, effacement, retrait du consentement, limitation, opposition aux décisions entièrement automatisées, portabilité et réclamation.

- Dans le portail : corriger votre profil, supprimer conversations, décisions et entrées du classeur, déconnecter tout outil connecté, délier WhatsApp et clôturer votre compte depuis la page Abonnement.
- Par courriel à privacy@pspsignaldesk.com depuis l'adresse de votre compte. Une demande qui parvient à une organisation partenaire est transmise à PSP le jour ouvré même.
- PSP accuse réception sous un jour et exécute l'accès, la rectification, la limitation, le retrait et l'effacement sur les systèmes de PSP sous trois jours.
- WhatsApp : répondez STOP ou BERHENTI à tout message, ou déliez le numéro dans le portail.

- Les réclamations sont adressées d'abord à PSP, puis à l'autorité de contrôle indiquée à la section 10.

7. En cas d'exposition de données personnelles

Une violation de données personnelles est tout événement par lequel des données personnelles sont perdues, altérées, divulguées ou consultées sans autorisation.

- PSP agit dès qu'une violation est suspectée : l'identifiant est changé, l'accès est fermé et les faits sont établis.
- Sous trois jours après confirmation, comme l'exigent l'article 46 de l'UU PDP et l'article 114 du PP 33/2026, PSP écrit à chaque abonné concerné par courriel dans sa langue et notifie l'autorité de contrôle. La notice indique quelles données sont concernées, quand et comment cela s'est produit, ce que PSP a fait, ce que vous devez faire et qui contacter.
- En cas d'impact public grave, PSP publie également un avis public.
- Les sous-traitants sont tenus par contrat d'informer PSP sans délai de tout incident de leur côté, et PSP suit alors les mêmes étapes.

Si vous suspectez un problème, écrivez à privacy@pspsignaldesk.com à tout moment ; vous recevez une réponse sous un jour.

8. Transferts transfrontaliers

Les données des abonnés sont traitées sur le réseau mondial de Cloudflare et par les sous-traitants de la section 3 aux États-Unis et en Irlande. Pour les abonnés en Indonésie, la base au titre de l'article 56 de l'UU PDP est celle des garanties adéquates et contraignantes : un accord de traitement des données avec chaque sous-traitant, des clauses d'absence d'entraînement lorsque l'IA est impliquée, un traitement lié aux instructions, la suppression sur demande et la notification des incidents. Pour les abonnés de l'Union européenne, du Royaume-Uni, d'Australie et de Singapour, les transferts vers ces sous-traitants reposent sur les mêmes accords, sur les clauses contractuelles types des sous-traitants et, lorsqu'ils la détiennent, sur leur certification au Cadre de protection des données UE-États-Unis. La Politique de confidentialité vous en informe avant l'activation.

9. Desks d'administration des partenaires

Lorsqu'une organisation partenaire met la plateforme à la disposition de ses membres, les agents qu'elle désigne voient, pour les membres de ce partenaire uniquement :

- Adresse électronique, organisation, langue, formule, statut, et si le membre a choisi une vue, choisi un assistant et relié WhatsApp (oui ou non seulement).
- Compteurs d'utilisation mensuels : analyste, documents, WhatsApp, site, podcast.
- Tickets d'assistance ouverts par les membres et leur résolution.
- Demandes de session et de formation : type, date, format et statut.

- Résultats d'enquête agrégés, et contenu éditorial publié dans le cadre du programme du partenaire.

Les agents du partenaire ne peuvent pas voir :

- Les conversations avec l'analyste, les décisions enregistrées ou le contenu du classeur.
- Les données des outils connectés ni aucun identifiant.
- Les documents téléversés.
- Les numéros WhatsApp ou le texte des messages.
- Les mots de passe, codes de connexion ou jetons de session.
- Les données d'abonnés hors du programme du partenaire.

Le partenaire utilise ces informations uniquement pour faire fonctionner son programme et ne les combine pas avec ses registres généraux de membres, sauf pour confirmer l'adhésion. Chaque action sur le desk d'administration est journalisée avec le compte de l'agent et l'heure.

10. Où vous êtes et la loi applicable

Les mêmes protections décrites dans cette déclaration s'appliquent à chaque abonné, où qu'il soit. Ce qui change, c'est la loi que vous pouvez invoquer et le régulateur auquel vous pouvez vous adresser.

Indonésie. PT Pacific Strategy Partners est le responsable du traitement au titre de l'UU PDP et du règlement gouvernemental 33/2026, et PSP SignalDesk est enregistré comme opérateur de système électronique de portée privée (PSE Lingkup Privat) au titre du règlement gouvernemental 71/2019, Tanda Daftar PSE 029810.01/DJAI.PSE/09/2026. Les demandes de droits sont exécutées sous trois jours et les violations notifiées sous trois jours. Le délégué à la protection des données est joignable à privacy@pspsignaldesk.com, avec une personne de contact domiciliée en Indonésie. Le régulateur est le ministère de la Communication et des Affaires numériques jusqu'à la constitution de l'Autorité de protection des données personnelles.

Australie. Pacific Strategy Partners, Sydney, applique les Australian Privacy Principles au titre du Privacy Act 1988 et le dispositif Notifiable Data Breaches, selon lequel une violation éligible est notifiée aux personnes concernées et à l'Office of the Australian Information Commissioner. Le régulateur est l'OAIC.

Singapour. Les abonnés à Singapour disposent des droits prévus par le Personal Data Protection Act 2012, dont l'accès, la rectification et le retrait du consentement. Le régulateur est la Personal Data Protection Commission.

Union européenne et Royaume-Uni. Les abonnés de l'UE et du Royaume-Uni disposent des droits prévus par le RGPD et le UK GDPR, auxquels cette déclaration satisfait, avec une violation notifiée à l'autorité de contrôle compétente sous 72 heures lorsque la loi l'exige. Les transferts vers nos sous-traitants reposent sur leurs clauses contractuelles types et, lorsqu'ils la détiennent, sur leur certification au Data Privacy Framework.

États-Unis et ailleurs. Les abonnés aux États-Unis, dans les autres pays de l'ASEAN, au Japon et dans tout autre pays bénéficient pleinement des protections de cette déclaration. Lorsque votre loi nationale vous confère un droit supplémentaire, nous l'honorons sur demande.

Langue. Pour les comptes en Indonésie, le texte en bahasa Indonesia de cette déclaration fait foi, l'anglais en étant l'équivalent. Les éditions française, néerlandaise, allemande, espagnole, chinoise et japonaise sont des traductions de lecture ; en cas de divergence avec l'anglais, l'anglais prévaut.

11. Contact

privacy@pspsignaldesk.com pour les demandes relatives à la vie privée, le retrait du consentement, la révision humaine et les réclamations.

contact@pacificstrategypartners.com pour toute autre question. PT Pacific Strategy Partners, WTC 5, Jl. Jend. Sudirman, Jakarta. Pacific Strategy Partners, Sydney.